AMENDMENTS TO THE CLAIMS

Claims 1 - 48 were pending at the time the Office Action was issued.

Claims 1, 6, 17, 22, 33, and 44 have been amended.

Claim 36 has been cancelled

Claims 1 – 35 and 37 - 48 remain pending.

1. **(Currently Amended)** A method comprising:

receiving a manifest defining a plurality of code assemblies that are members of at least one application, wherein the manifest defines at least one trusted application and application evidence for making a trust decision;

evaluating the application evidence ~~for the at least one application~~ to determine if the at least one application is trusted; ~~and~~

generating a permission grant set for each code assembly that is a member of the at least one application if the application evidence satisfies at least one condition for trusting the at least one application; and

passing the permission grant to a run-time call stack.

2. **(Original)** The method of claim 1 further comprising evaluating application evidence for a group of applications and generating a permission grant set for each code assembly that is a member of the group of applications if the application evidence satisfies at least one condition for trusting the group of applications.

3. **(Original)** The method of claim 1 wherein evaluating application evidence is based at least in part on an XrML license.

4. **(Original)** The method of claim 1 further comprising evaluating application evidence at an application level and a code assembly level before trusting the at least one application.

5. **(Original)** The method of claim 1 further comprising evaluating application evidence at a group level, an application level, and a code assembly level before trusting the at least one application.

6. **(Currently Amended)** A method comprising:

generating a permission grant set for each code assembly that is a member of at least one application if application evidence for the at least one application satisfies at least one ~~trust~~ condition specified in a security policy specification for trusting the at least one application, wherein the security policy specification defines multiple policy levels; and

granting permissions on a computer system based on the permission grant set.

7. **(Original)** The method of claim 6 further comprising generating a

permission grant set for each code assembly that is a member of a group of applications if application evidence for the group of applications satisfies at least one trust condition.

8. **(Original)** The method of claim 6 further comprising determining if the code assembly is a member of the at least one application.

9. **(Original)** The method of claim 6 further comprising receiving a manifest defining members of the at least one application.

10. **(Original)** The method of claim 6 wherein satisfying at least one trust condition is based at least in part on evidence provided with the at least one application.

11. **(Original)** The method of claim 6 wherein satisfying at least one trust condition is based at least in part on evidence external to the at least one application.

12. **(Original)** The method of claim 6 wherein satisfying at least one trust condition is based at least in part on an XrML license.

13. **(Original)** The method of claim 6 wherein satisfying at least one

trust condition is based on evidence from user interaction.

14. **(Original)** The method of claim 6 wherein satisfying at least one trust condition is based on evidence from evaluation of previous trust decisions.

15. **(Original)** The method of claim 6 further comprising evaluating application evidence at an application level and a code assembly level before allowing the at least one application to execute.

16. **(Original)** The method of claim 6 further comprising evaluating application evidence at a group level, an application level, and a code assembly level before allowing the at least one application to execute.

17. **(Currently Amended)** A computer program product encoding a computer program for executing on a computer system a computer process, the computer process comprising:

receiving a manifest defining a plurality of code assemblies that are members of at least one application, wherein the manifest defines at least one trusted application and application evidence for making a trust decision;

evaluating the application evidence ~~for the at least one application~~ to determine if the at least one application is trusted; and

generating a permission grant set for each code assembly that is a member

of the at least one application if the application evidence satisfies at least one condition for trusting the at least one application.

18. **(Original)** The computer program product of claim 17 wherein the computer process further comprises evaluating application evidence for a group of applications and generating a permission grant set for each code assembly that is a member of the group of applications if the application evidence satisfies at least one condition for trusting the group of applications.

19. **(Original)** The computer program product of claim 17 wherein the computer process further comprises evaluating application evidence based at least in part on an XrML license.

20. **(Original)** The computer program product of claim 17 wherein the computer process further comprises evaluating application evidence at an application level and a code assembly level before trusting the at least one application.

21. **(Original)** The computer program product of claim 17 wherein the computer process further comprises evaluating application evidence at a group level, an application level, and a code assembly level before trusting the at least one application.

22. **(Currently Amended)** A computer program product encoding a computer program for executing on a computer system a computer process, the computer process generating a permission grant set for each code assembly that is a member of at least one application if application evidence for the at least one application satisfies at least one ~~trust~~ condition specified in a security policy specification for trusting the at least one application, wherein the security policy specification defines multiple policy levels.

23. **(Original)** The computer program product of claim 22 wherein the computer process further comprises generating a permission grant set for each code assembly that is a member of a group of applications if application evidence for the group of applications satisfies at least one trust condition.

24. **(Original)** The computer program product of claim 22 wherein the computer process further comprises determining if the code assembly is a member of the at least one application.

25. **(Original)** The computer program product of claim 22 wherein the computer process further comprises receiving a manifest defining members of the at least one application.

26. **(Original)** The computer program product of claim 22 wherein the computer process is based at least in part on evidence provided with the at least one application.

27. **(Original)** The computer program product of claim 22 wherein the computer process is based at least in part on evidence external to the at least one application.

28. **(Original)** The computer program product of claim 22 wherein the computer process is based at least in part on an XrML license.

29. **(Original)** The computer program product of claim 22 wherein the computer process is based on evidence from user interaction.

30. **(Original)** The computer program product of claim 22 wherein the computer process is based on evidence from evaluation of previous trust decisions.

31. **(Original)** The computer program product of claim 22 wherein the computer process further comprises evaluating evidence at an application level and a code assembly level before executing the at least one application.

32. **(Original)** The computer program product of claim 22 wherein the computer process further comprises evaluating evidence at a group level, an application level, and a code assembly level before executing the at least one application.

33. **(Currently Amended)** A system comprising:

a manifest defining at least one application;

application evidence [[for]] to determine whether the at least one application is trusted; and

a policy manager to evaluate ~~evaluating~~ the application evidence relative to at least one condition ~~for trusting the at least one application~~, wherein the policy manager generates a permission grant set for each code assembly that is a member of the at least one application if the application evidence satisfies the at least one condition specified in a security policy specification for trusting the at least one application, wherein the security policy specification defines multiple policy levels, and wherein permissions are granted on a computer system based on the permission grant set.

34. **(Original)** The system of claim 33 further comprising an XrML program authorization module operatively associated with the policy manager for evaluating application evidence including at least one XrML license.

35. **(Original)** The system of claim 33 wherein the policy manager evaluates evidence at a group level, an application level, and a code assembly level before the at least one application is executed.

36. **(Cancelled)**

37. **(Original)** The system of claim 33 wherein the policy manager further determines if the code assembly is a member of the at least one application.

38. **(Original)** The system of claim 33 wherein the application evidence is provided with the at least one application.

39. **(Original)** The system of claim 33 wherein the application evidence is provided external to the at least one application.

40. **(Original)** The system of claim 33 wherein the application evidence includes at least an XrML license.

41. **(Original)** The system of claim 33 wherein the application evidence includes evidence provided via user interaction.

42. **(Original)** The system of claim 33 wherein the application

evidence includes evidence from the evaluation of previous trust decisions.

43. **(Original)** The system of claim 33 further comprising a security policy specification defining at least one trust condition for an application component, wherein the policy manager evaluates the at least one trust condition in the security policy specification.

44. **(Currently Amended)** A computer-readable medium having stored thereon a data structure, comprising:

a first data field specifying members of at least one application;

a second data field containing application evidence to evaluate whether ~~associated with~~ the at least one application is trusted, wherein permission grant sets are generated for each member of the at least one application ~~based on~~ if the application evidence satisfies at least one condition specified in a security policy specification for trusting the at least one application, wherein the security policy specification defines multiple policy levels.

45. **(Original)** The data structure of claim 44 wherein the first data field defines a group of applications.

46. **(Original)** The data structure of claim 44 further comprising a third data field identifying a location of one of the members of the at least one

application.

47. **(Original)** The data structure of claim 44 further comprising a third data field specifying a requested level of trust for the at least one application.

48. **(Original)** The data structure of claim 44 further comprising a third data field requesting different levels of trust for different members of the at least one application.